Chapter 21: Virtual Network Manager - VNet Peering

Introduction

Figure 21-1 shows a small-size Azure hub and spoke deployment. While configuring VNet peering connections one at a time may not be overly challenging, the task becomes time-consuming and prone to errors when dealing with numerous VNets—imagine having tens or even hundreds of them. Even if you utilize ARM templates, Bicep, or other automation tools, you must execute the process when creating a new VNet peering connection.

This chapter explains how to utilize an Azure Virtual Network Manager (VNM) for effectively managing VNet peering connections in large-scale VNet deployments. Figure 21-1 illustrates the building blocks and configuration steps using VNM to deploy dynamic VNet peering connections. First, we create a VNM instance and define its scope, our subscription on this example. Next, we define a Network Group (NG) and associate our spoke VNets with it. This chapter explains both manual and dynamic, policy-based assignment options. Once we have created an NG, we build a connection configuration, informing the VNM about our intention to deploy a Hub and Spoke topology with "vnet-hub" serving as the Hub and our newly created NG as the spoke Network Group. Lastly, we deploy the configuration within our region.

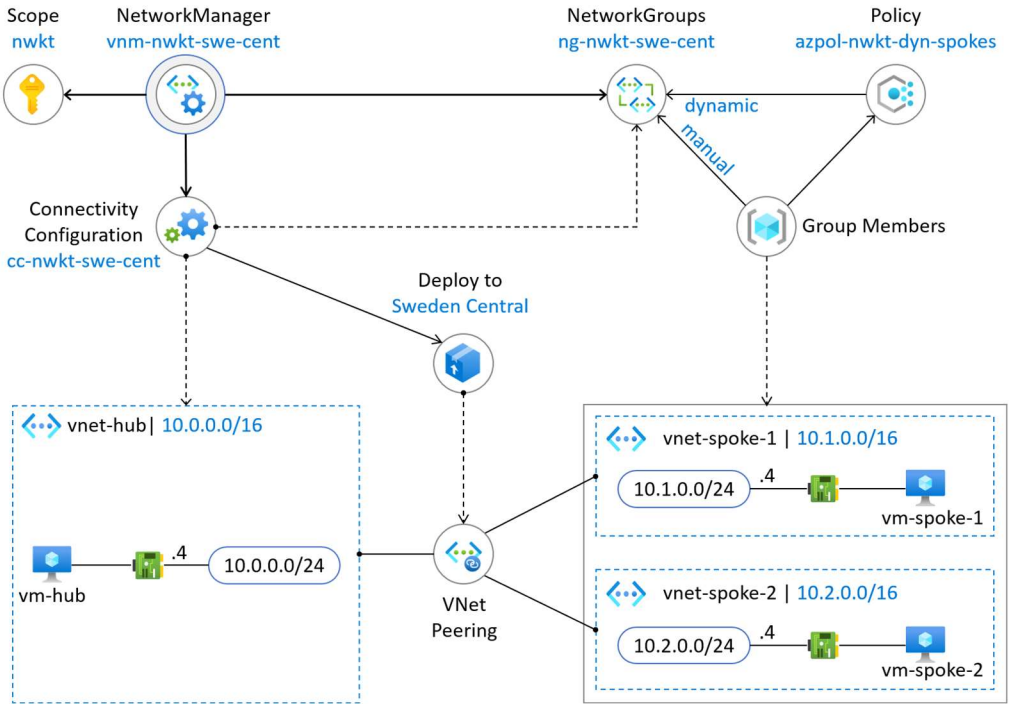

Figure 21-1: *ILB Example Topology.*

Create Virtual Network Manager

Select the *Create a resource* from the Azure portal home view. Type the *Network Manager* on the search field. Next, select Microsoft's Network Manager and click the *Create* button.

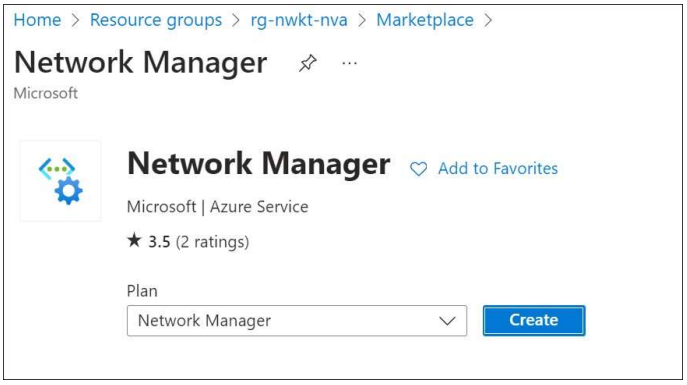

Figure 21-2: *Create a Network Manager.*

First, select the subscription and resource group from the drop-down menus. Then fill in the Name field (vnm-nwkt-net-mgmt) and choose a region from the drop-down menu. Select the Connectivity, Security admin option from the drop-down list. Next, go to the Management scope tab.

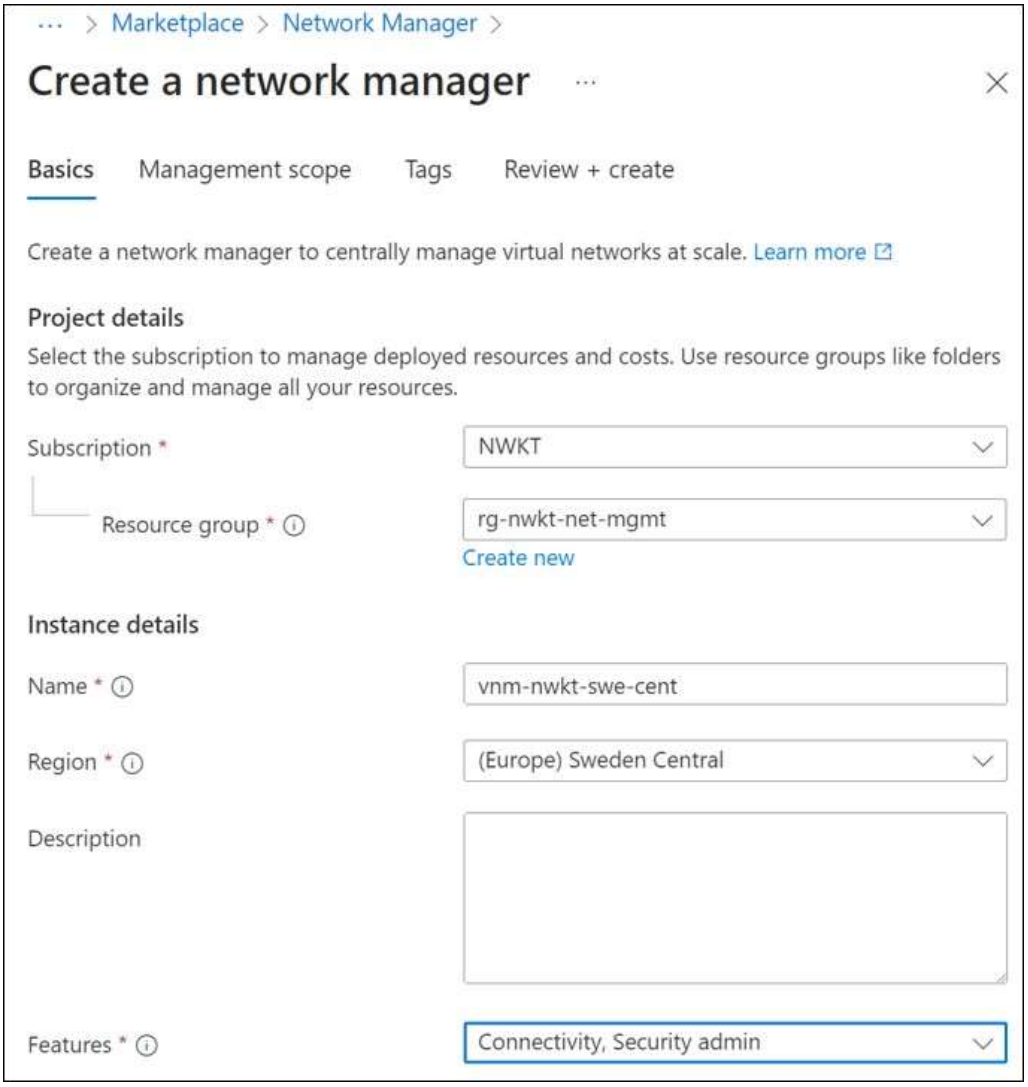

Figure 21-3: *Create a Network Manager – Basic Information.*

Click the "+Add" button in the Management scope tab.

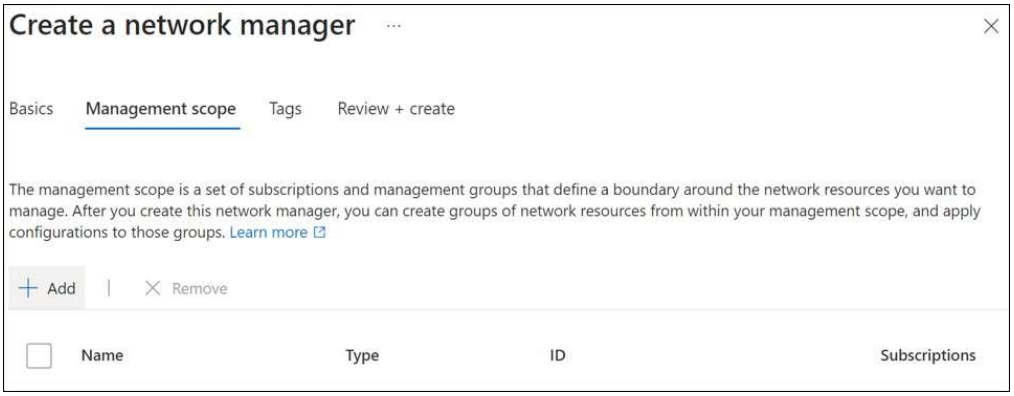

Figure 21-4: *Create a Network Manager – Select Management Scope.*

The scope can be Subscription or Management Group. We are using a subscription in this example. After selecting your subscription, click the Select button.

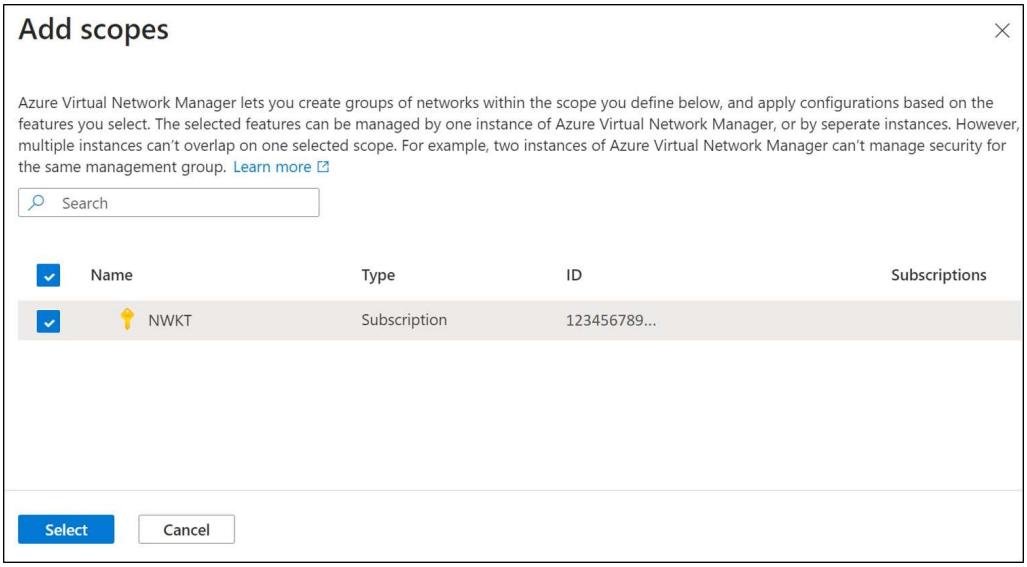

Figure 21-5: *Create a Network Manager – Select Management Scope: Subscription.*

Select the “Create” button in the "Review + Create" tab for deploying the new Virtual Network Manager.

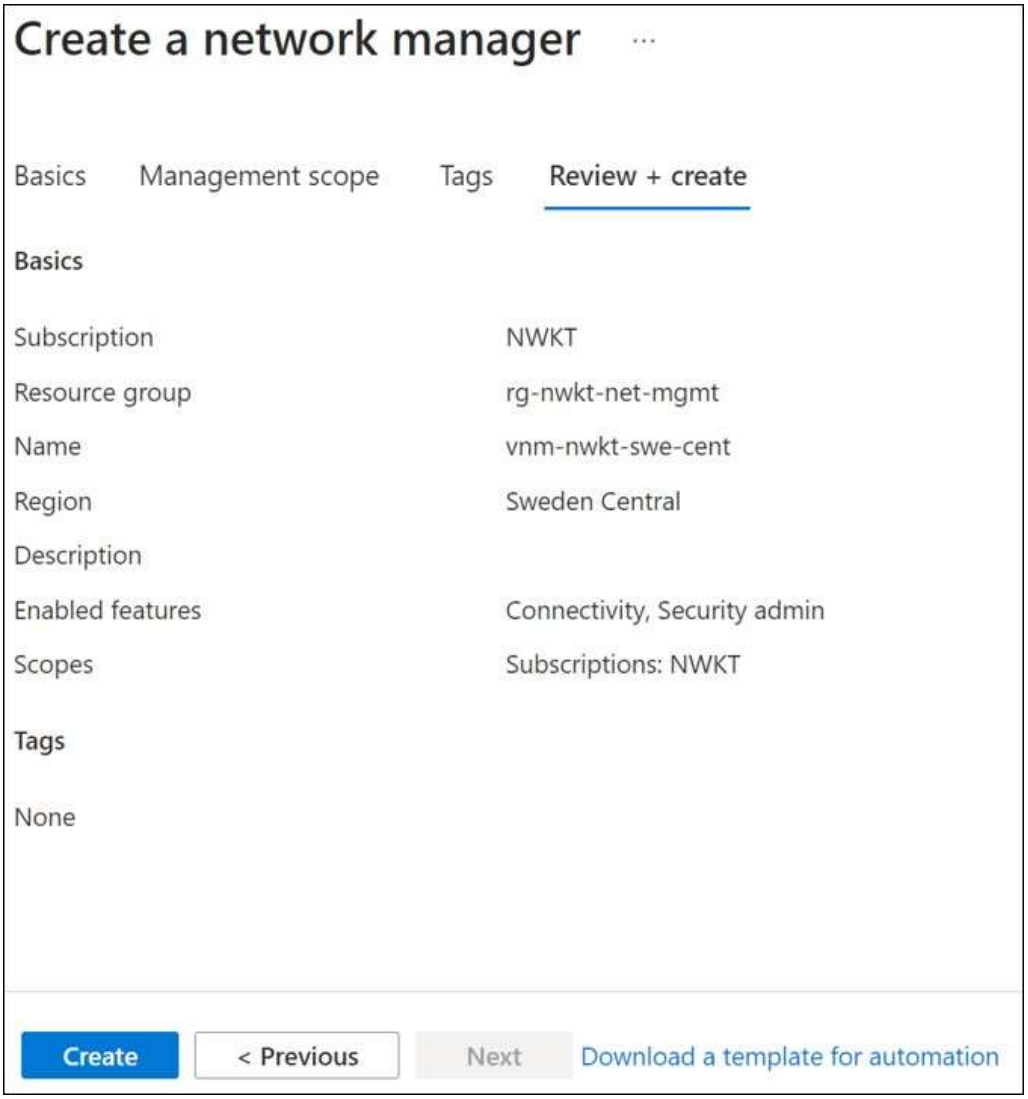

Figure 21-6: *Create Network Manager – Deployment.*

Figure 21-7 shows an Overview of Virtual Network Manager vnm-nwkt-swe-cent.

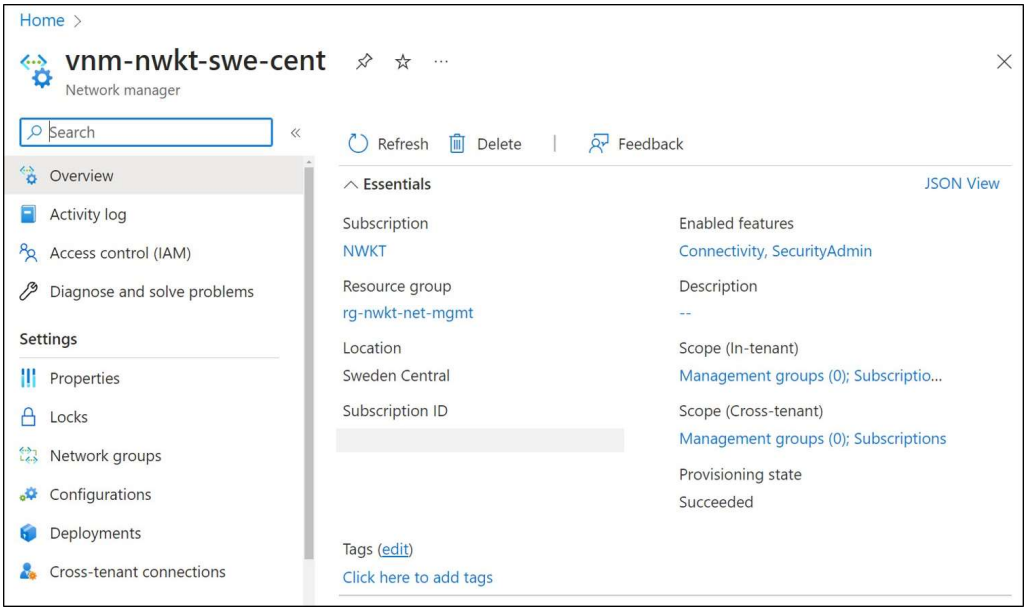

Figure 21-7: *An Overview of Network Manager.*

The figure below illustrates the Network Manager deployment Progress.

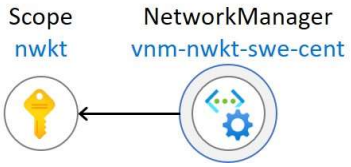

Figure 21-8: *Implementation Progress.*

Create Network Group

Select the Network Group option from the Settings section on the left pane in Network Manager main view (Figure 21-9). Create a new Network Group by clicking the Create button.

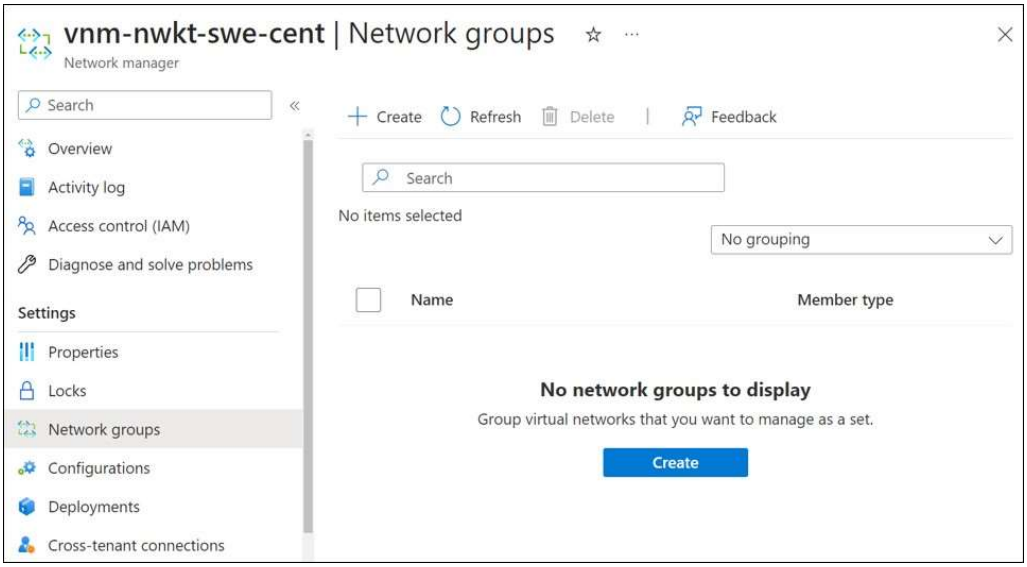

Figure 21-9: *Create Network Group – Step#1.*

Name the Network Group and describe it if you like. To proceed, click the Create button.

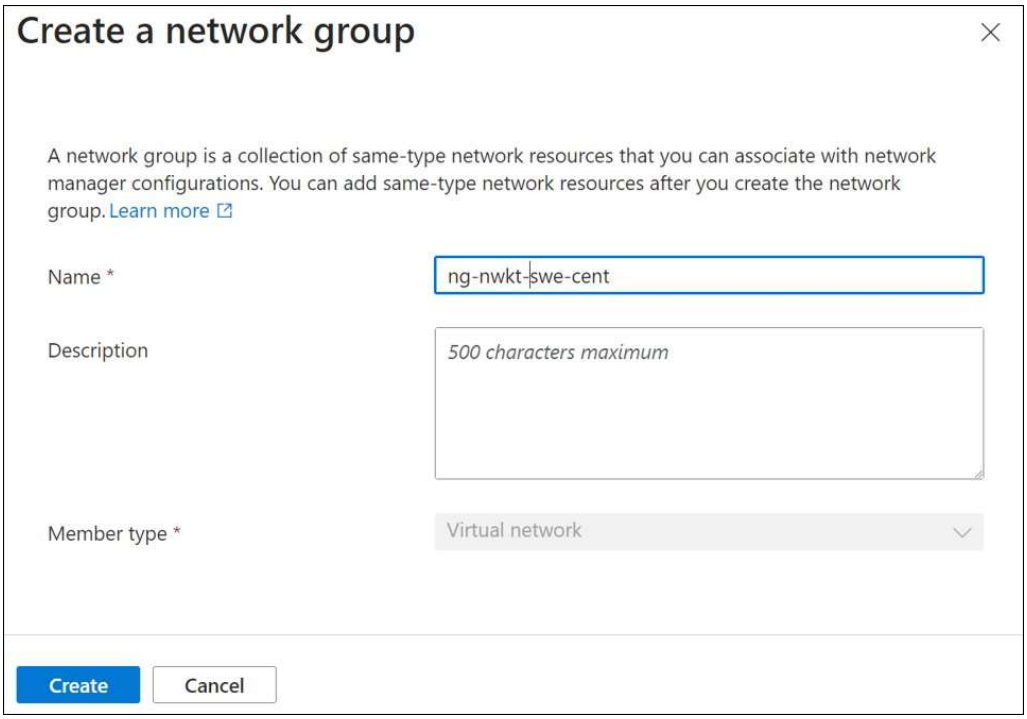

Figure 21-10: *Create Network Group – Step#2.*

The Network Manager main view now shows our new Network Group ng-nwkt-swe-cent. As the next step, we add Virtual Networks manually to it. First, choose the Network Groups (NG) under the Network Manager's Setting section. Then, Select your NG from the right pane.

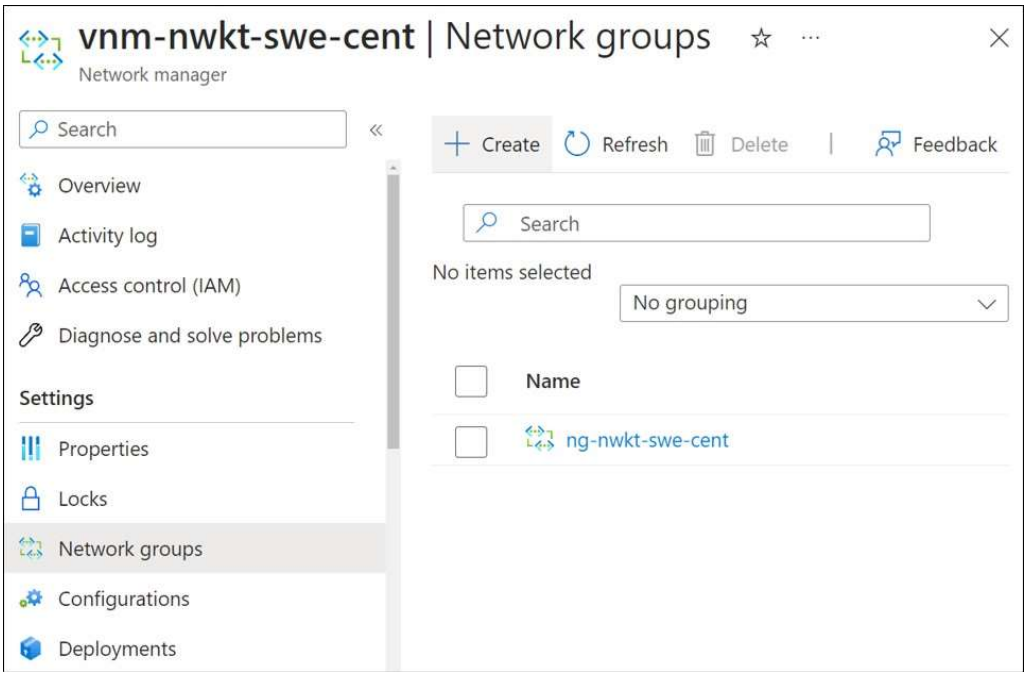

Figure 21-11: *Add Virtual Network to Network Group Manually – Step#1.*

Click the *Add virtual networks* button to define which VNets you want to attach to NG (Figure 21-12).

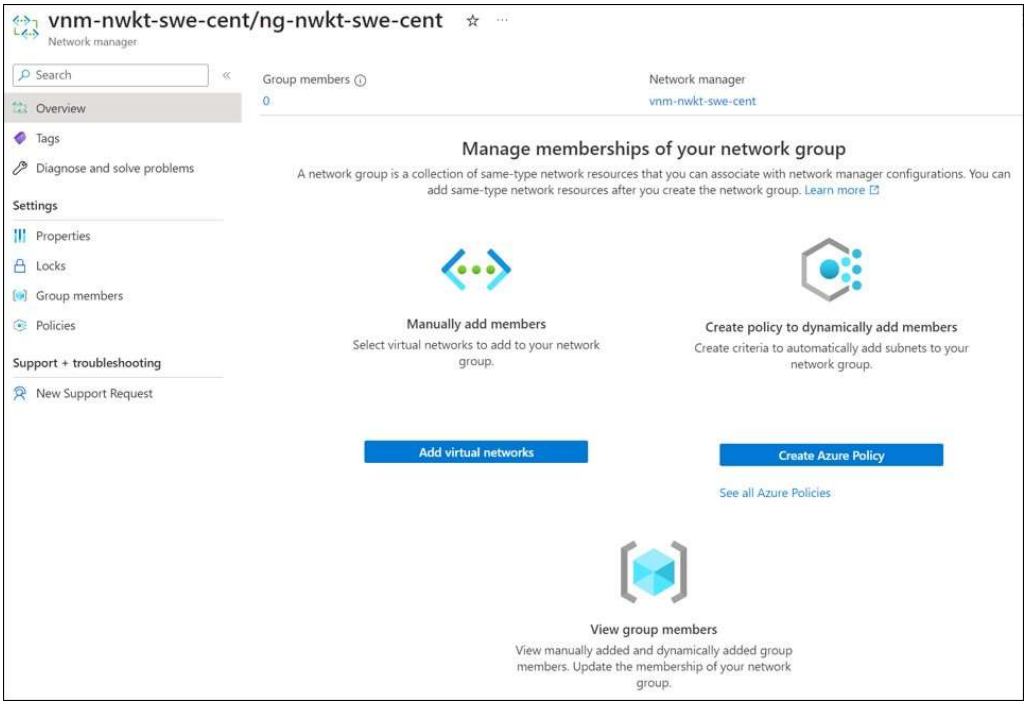

Figure 21-12: *Add Virtual Network to Network Group Manually – Step#2.*

At this phase, we have only two spoke VNets, which we add to NG. Do not select the VNet that you are using as hub VNet. We add the third spoke VNet when explaining the automatic, policy-based VNet-to-NG assignment.

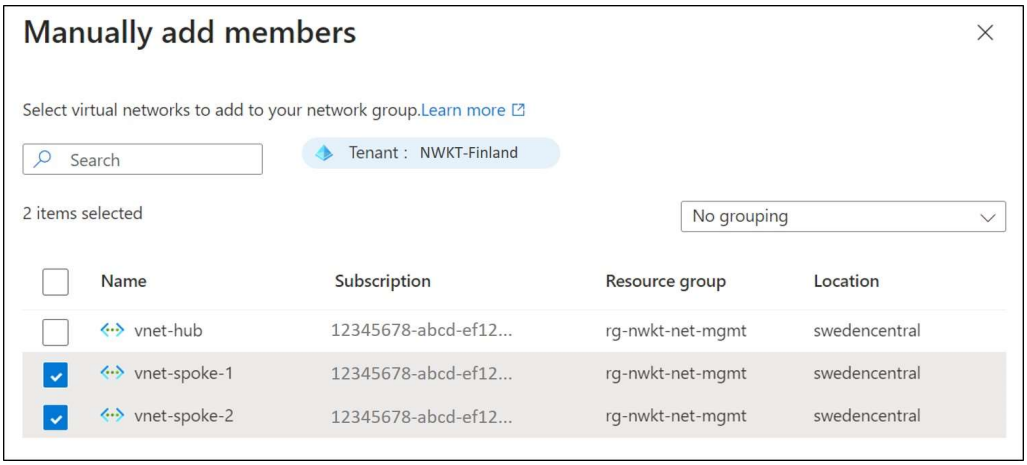

Figure 21-13: *Add Virtual Network to Network Group Manually – Step#3.*

Figure 21-14 shows that we have added vnt-spoke-1 and vnet-spoke-2 to NG ng-nwkt-swe-cent.

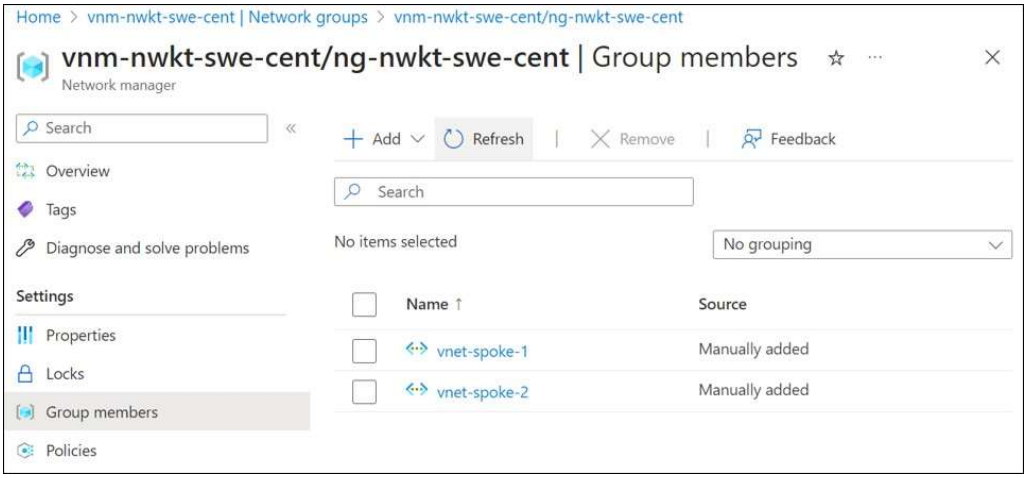

Figure 21-14: *Add Virtual Network to Network Group Manually – Step#4.*

Figure below illustrates our progress.

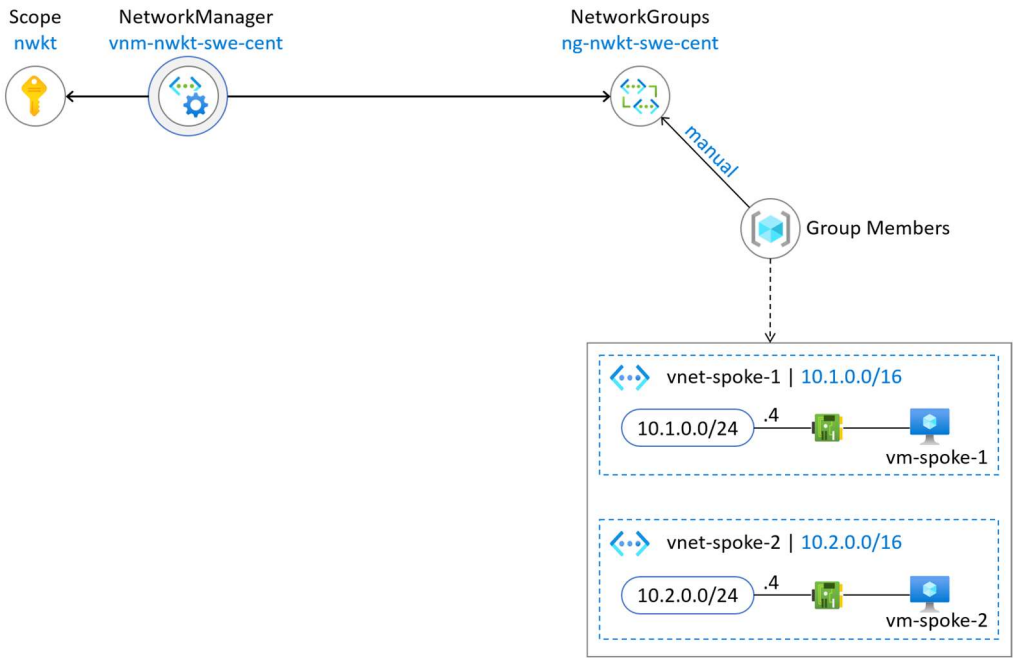

Figure 21-15: *Implementation Progress.*

Create Connectivity Configuration

Now, we have associated spoke VNets with the NG. Next, we build up a *Connectivity configuration (CC)* that defines the topology, in our example Hub-and-Spoke, and sets the hub and Spoke VNets. When we later deploy the CC, it creates bi-directional VNet peering connections between the VNets. Start by selecting the *Configuration* options under the *Settings* section and click the *Create connectivity configuration* button (Figure 21-16). In the *Basics* tab, name the CC (Figure 21-17).

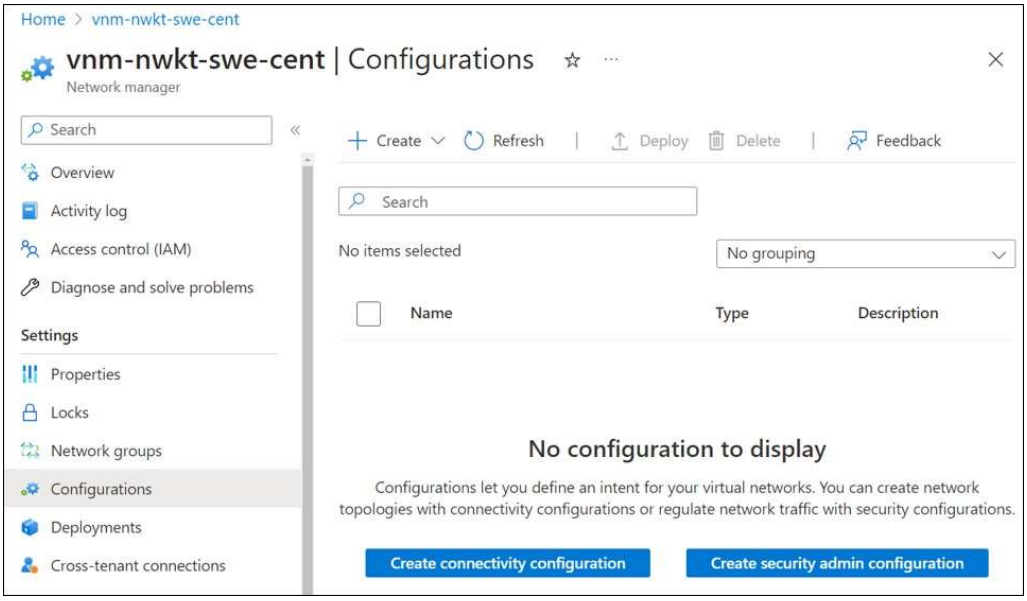

Figure 21-16: *Build a Connectivity Configuration – Step#1.*

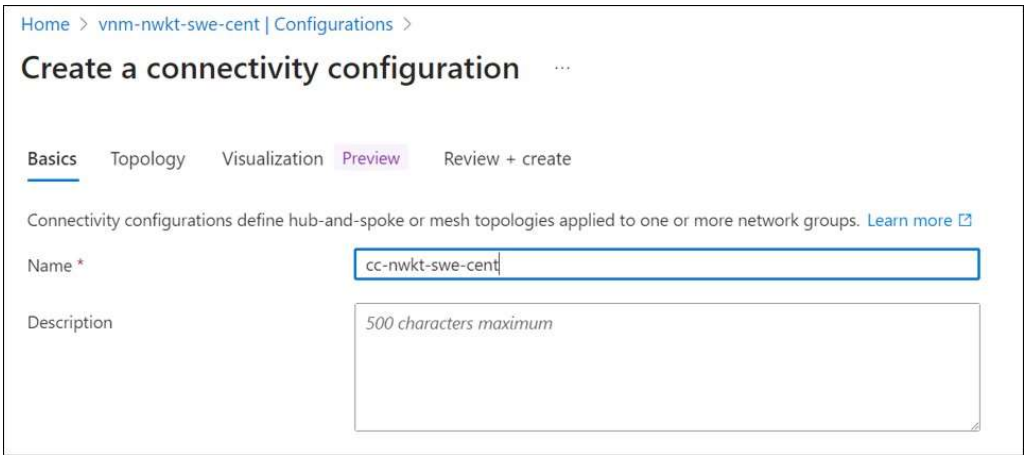

Figure 21-17: *Build a Connectivity Configuration – Step#2.*

In the *Topology* tab, you first select the hub VNet. First, select the *Hub and Spoke* radio button and then click the *Select a hub* hyperlink. It opens a window where you choose your hub VNet.

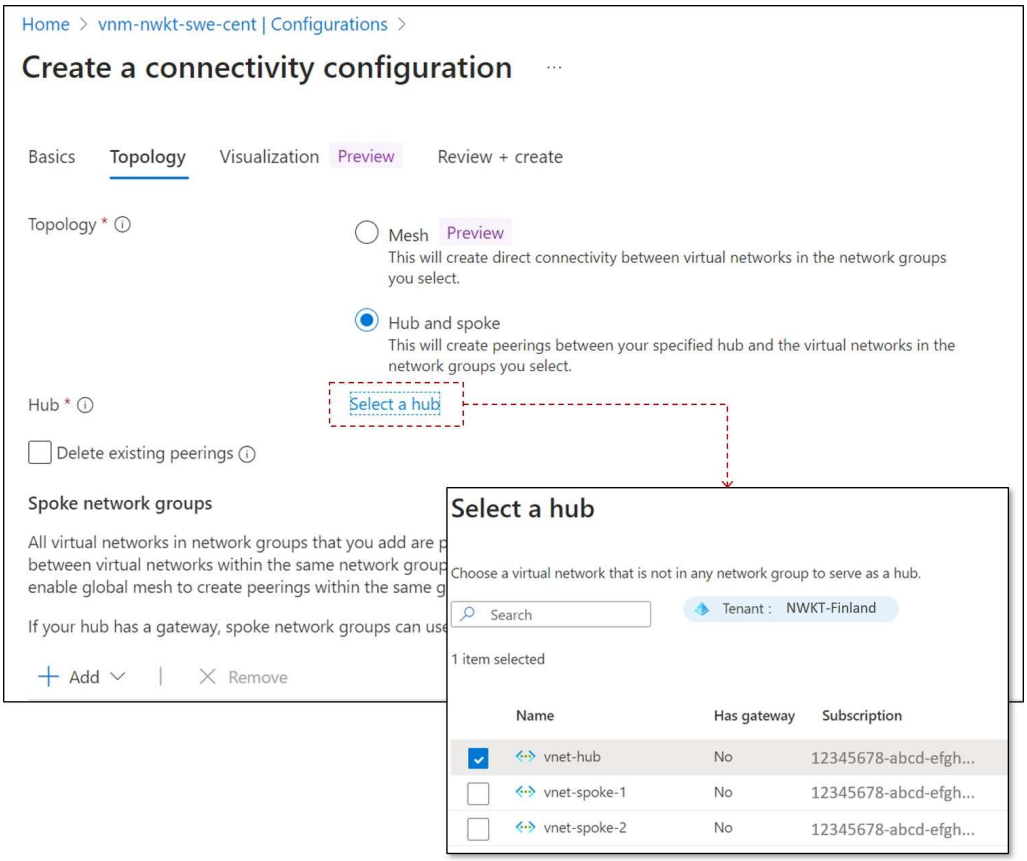

Figure 21-18: *Build a Connectivity Configuration – Select Hub VNet.*

After selecting the hub VNet, click the + *Add* button and click the *Add network groups* hyperlink. It opens an *Add network groups* window, where you can choose the previously created NG or create a new one.

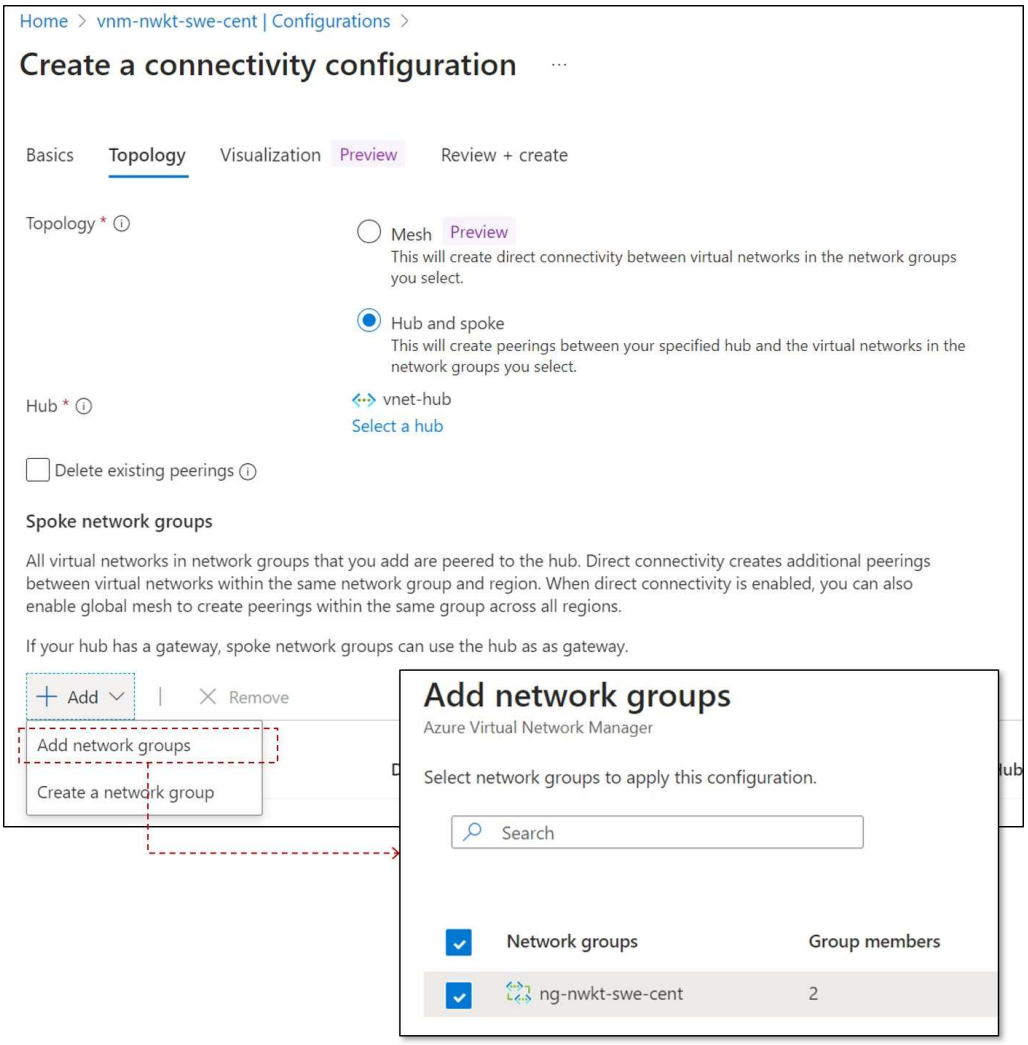

Figure 21-19: *Build a Connectivity Configuration – Select Network Group.*

Figure 21-20 verifies that the configuration builds up a hub-and-spoke topology using VNet vnet-hub as a hub and VNets we have associated to Network Group ng-nwkt-swe-cent.

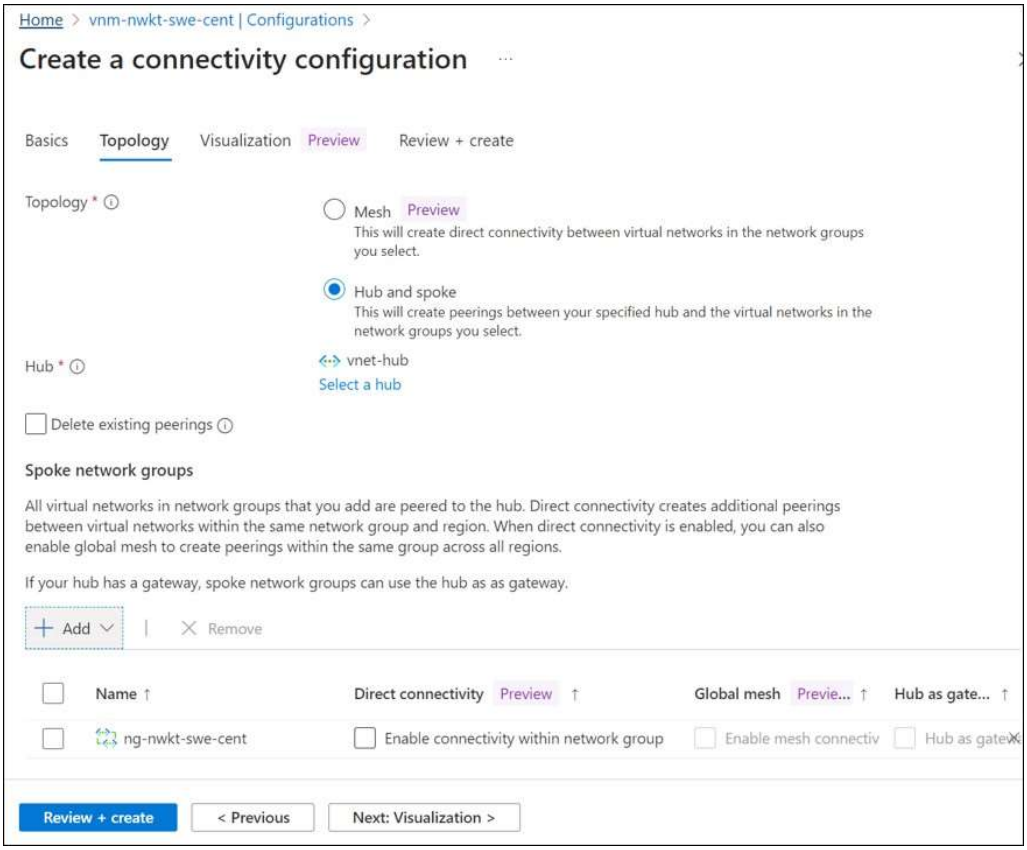

Figure 21-20: *Build a Connectivity Configuration – Hub and Spoke Selections.*

Figure 21-21 on the next page shows the *Visualization* tab, where you can see the topology you are deploying. Go to the *Review + create* window and click the *Create* button (Figure 21-22).

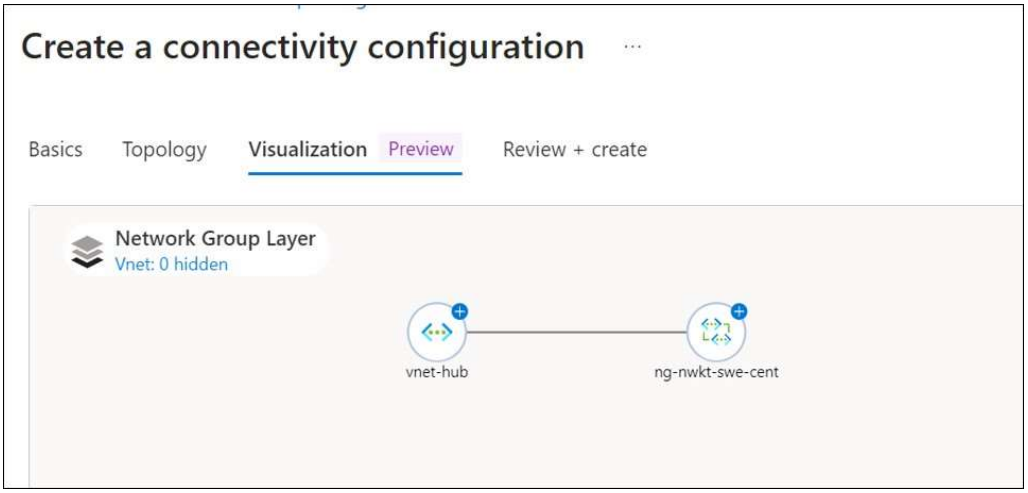

Figure 21-21: *Build a Connectivity Configuration – Visualization.*

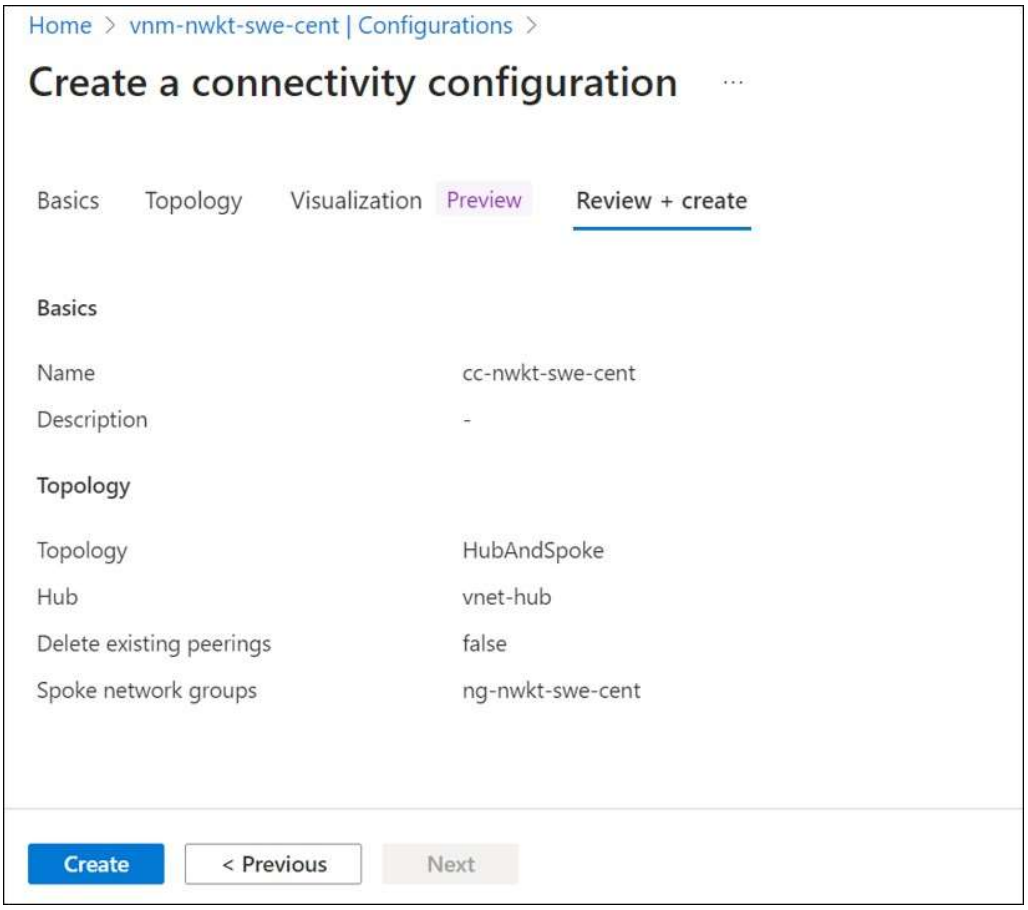

Figure 21-22: *Build a Connectivity Configuration – Deployment.*

Figure below illustrates our progress.

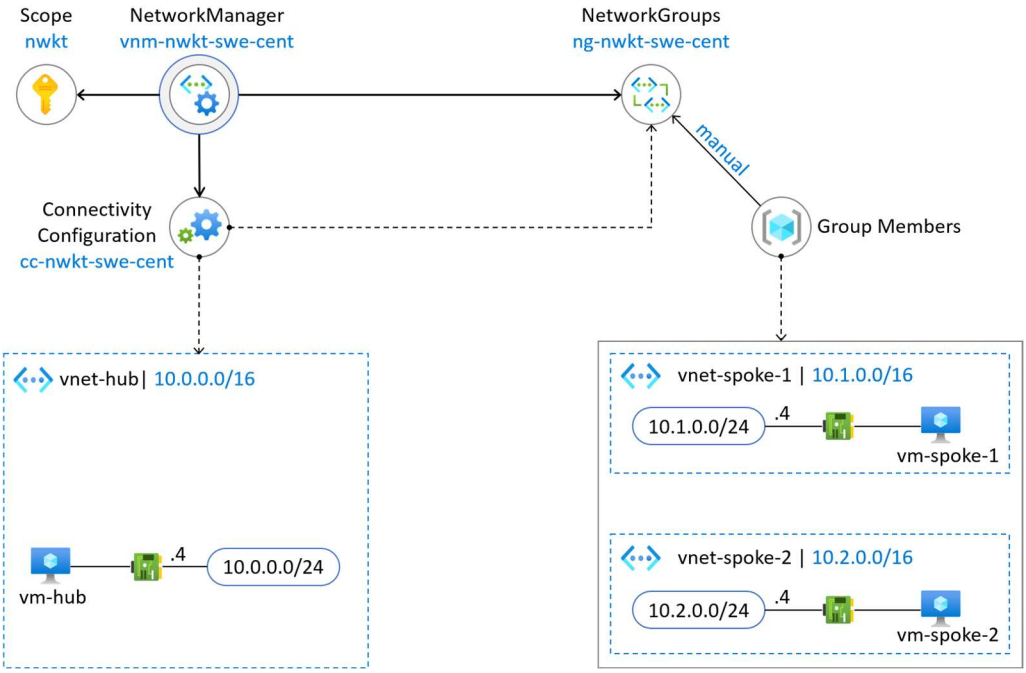

Figure 21-23: *Implementation Progress.*

Deploy Connectivity Configuration

As the final step, we deploy the connectivity configuration. Select the Deployment option from the Settings section and click the Deploy configuration.

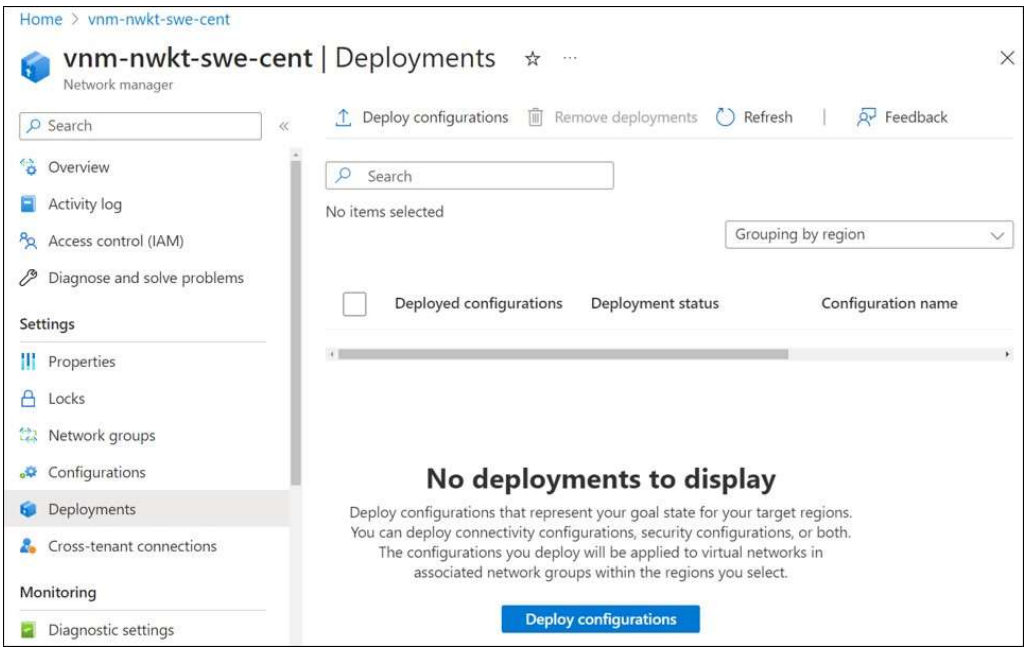

Figure 21-24: *Connectivity Configuration Deployment.*

Select your configuration and Target region from the drop-down menus, and proceed to the Review + Deploy tab. The Review view shows the existing configuration and the new one. By clicking the Deploy button, Azure creates bi-directional VNet peerings.

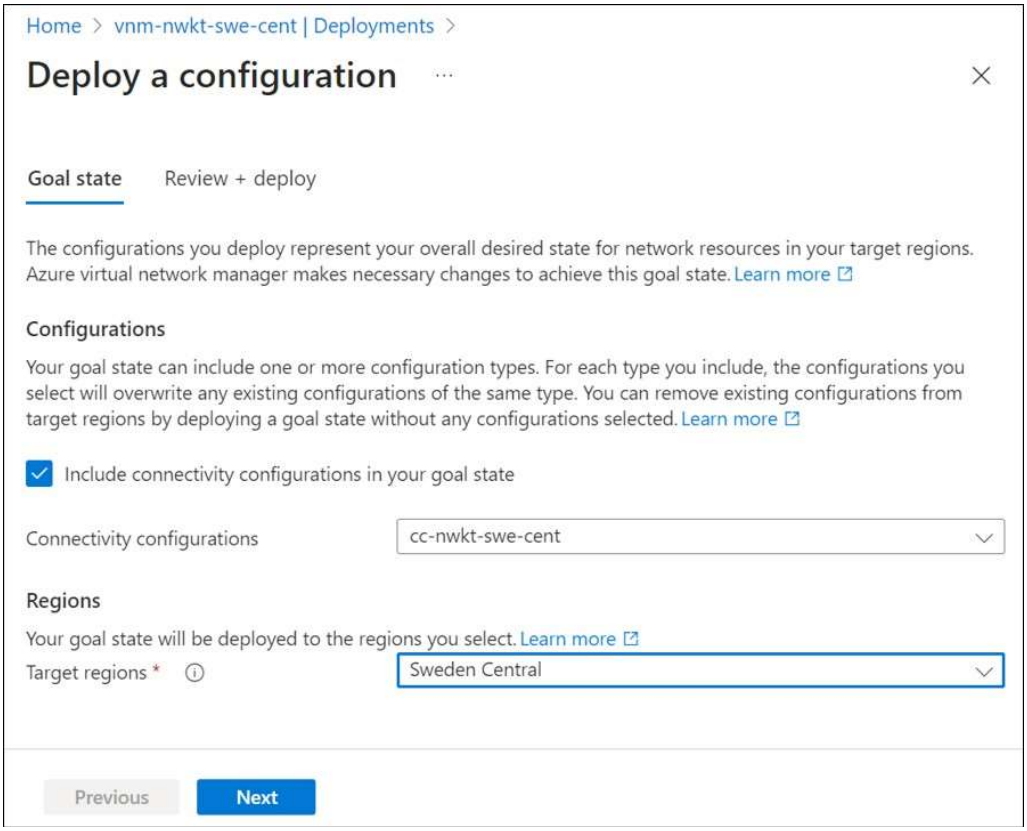

Figure 21-25: *Connectivity Configuration Deployment.*

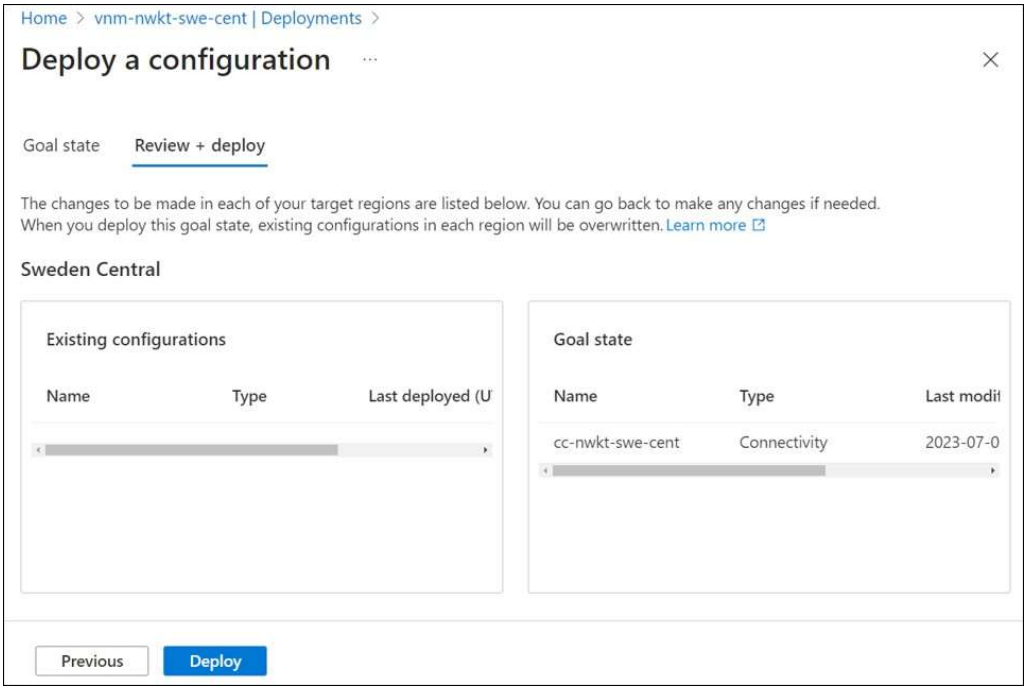

Figure 21-26: *Connectivity Configuration Deployment.*

After the configuration deployment is ready, go to Virtual Network Manager and select the Deployments option under the Settings section. There we can see that the status of the deployment shows "Succeeded."

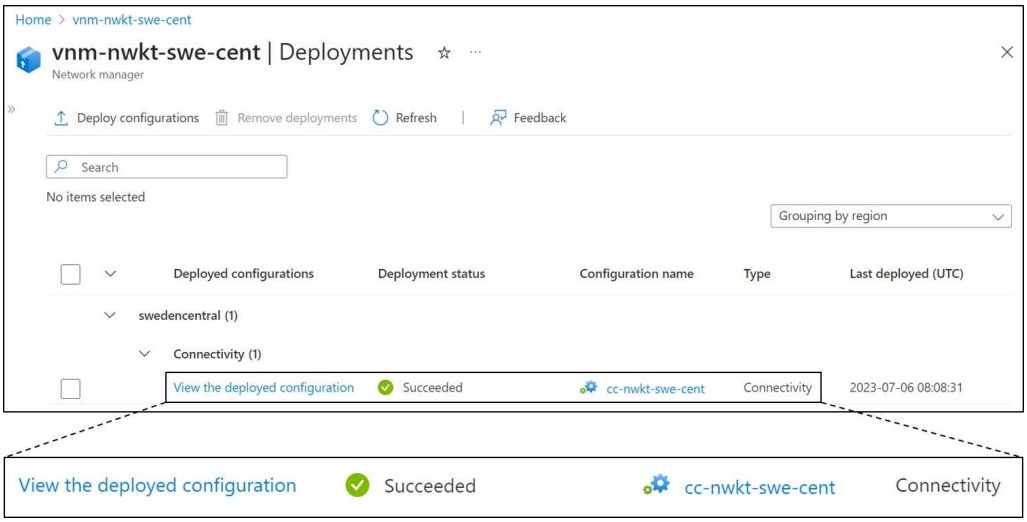

Figure 21-27: *Connectivity Configuration Deployment - Verification.*

Figures 21-28 and 21-29 show the VNet peering information Azure has created for vnet-hub and vnet-spoke-1.

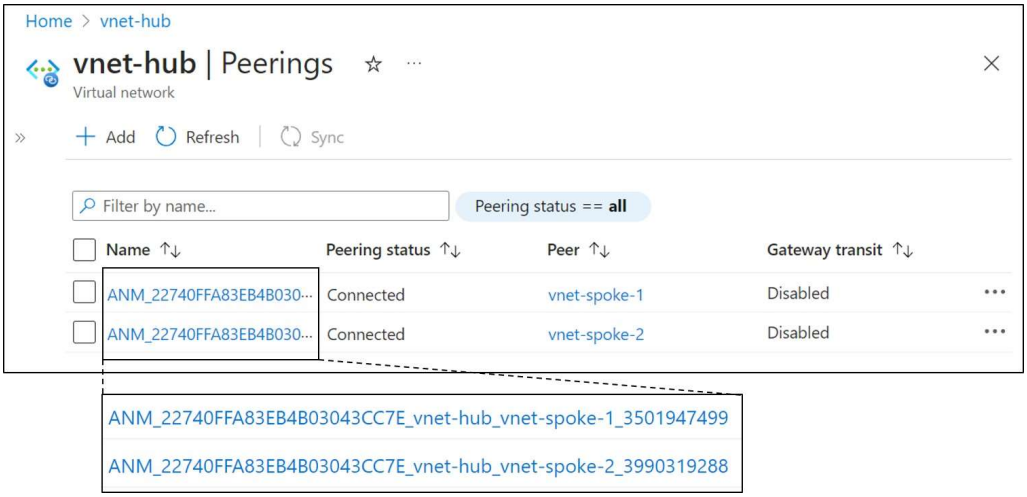

Figure 21-28: *VNet Peering Verification from the VNet vnet-hub.*

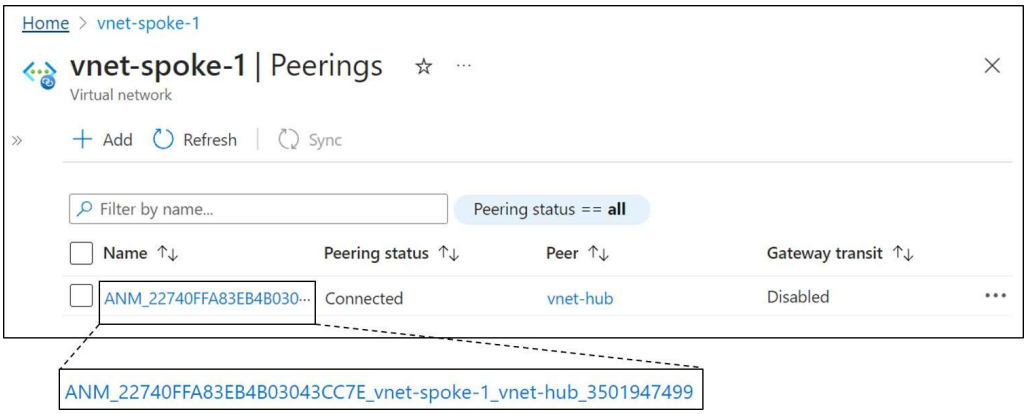

Figure 21-29: *VNet Peering Verification from the VNet vnet-spoke-1.*

You can view the detailed peering settings by clicking the peering name hyperlink (Figure 21-30).

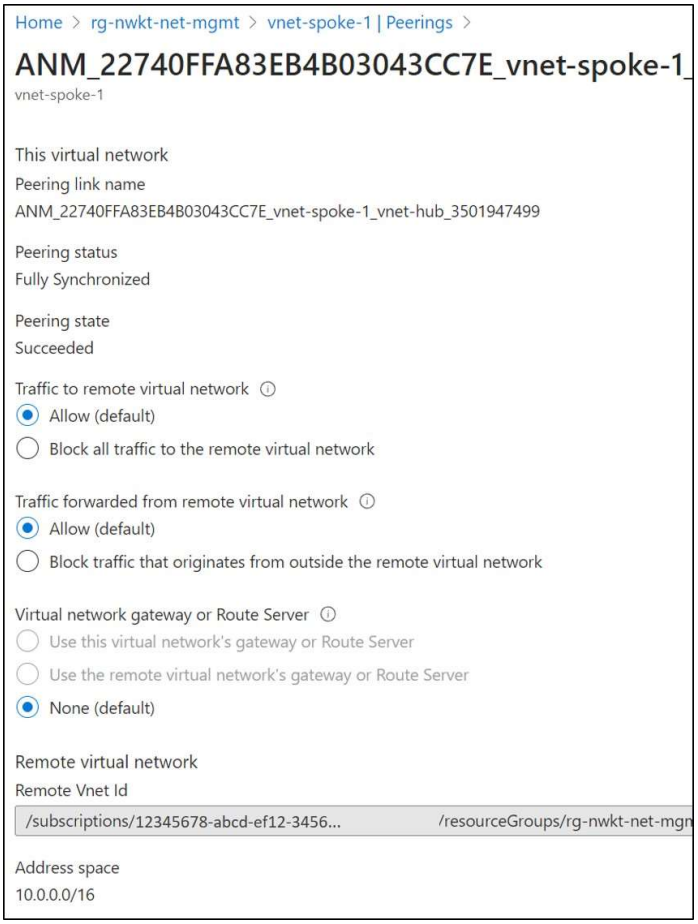

Figure 21-30: *VNet Peering Settings.*

You can view the configuration deployed using Virtual Network Manager by selecting the Network Manager option from the Settings section in VNet main view.

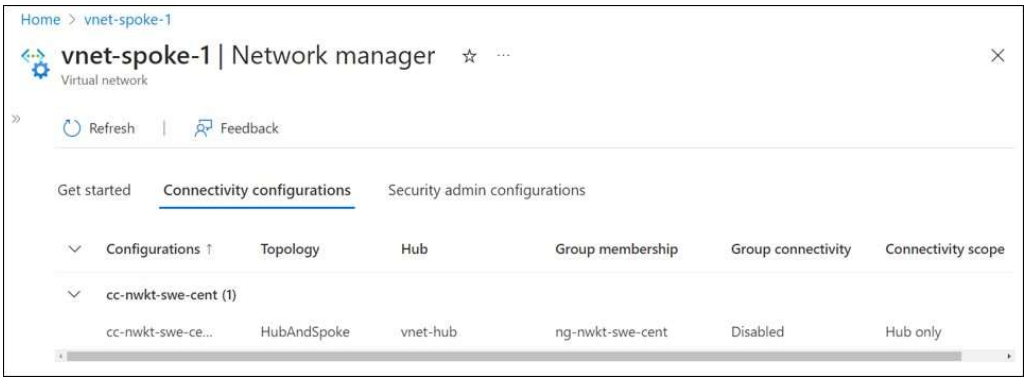

Figure 21-31: *VNet vnet-spoke-1 Network Manager.*

Figure 21-32 depicts the complete deployment.

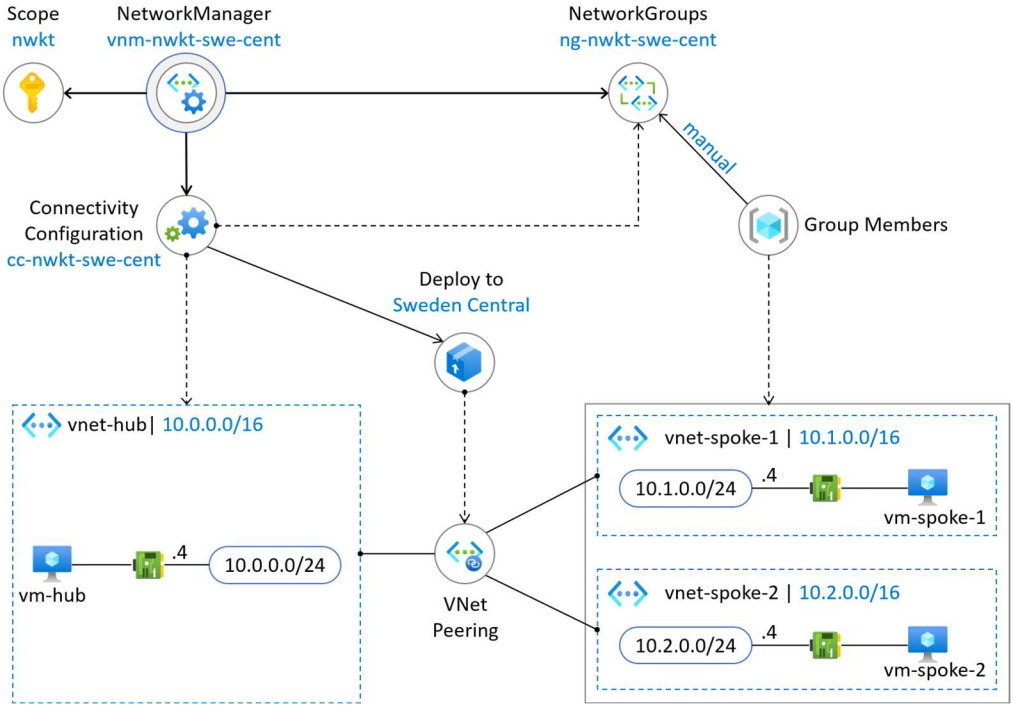

Figure 21-32: *Deployed Topology.*

Add VNets Dynamically to Network Group

We can add Virtual Networks dynamically to Network Group (NG) using Azure Policies. Figure 21-33 depicts an Azure Policy that adds all VNets having the word spoke in their name to Network Group. It adds existing VNets vnet-spoke-1 and vnet-spoke-2 to NG. Then we deploy the third VNet, vnet-spoke-3, which the policy automatically assigns to NG.

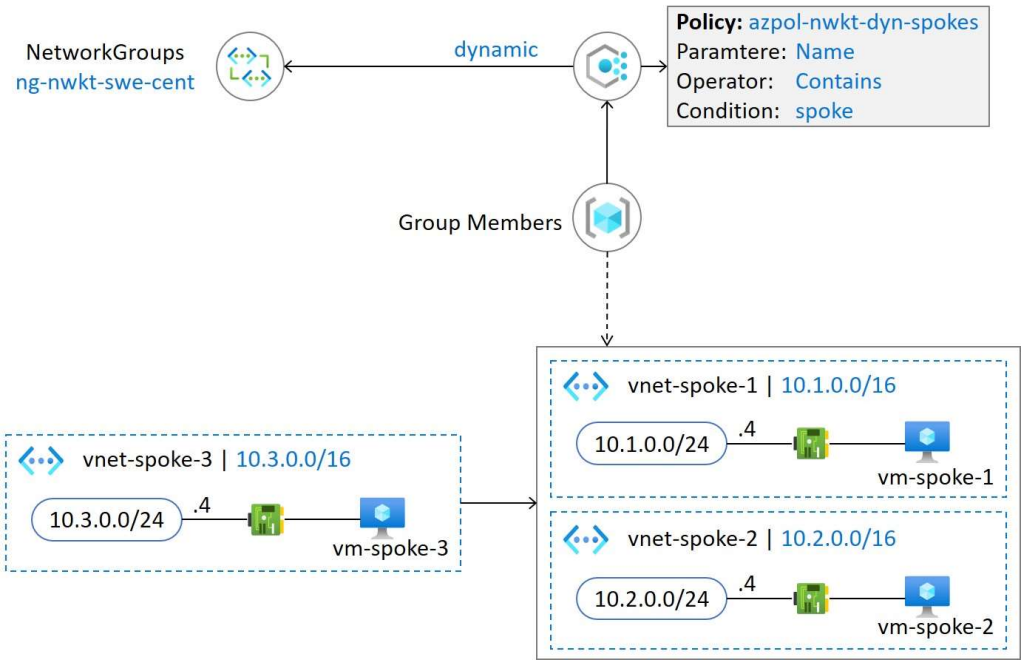

Figure 21-33: *Azure Policy for Network Group Members.*

Start the policy deployment by selecting the *Group members* option from the Settings section. Then, click the *Create Azure Policy* button.

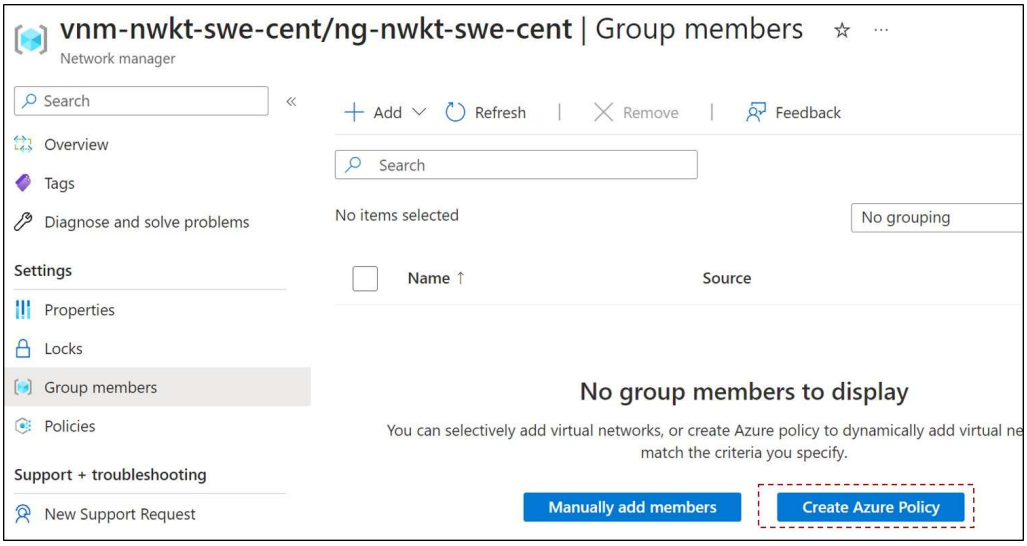

Figure 21-34: *Create Azure Policy.*

Our intent is to dynamically add all existing and new spoke VNets to a hub and spoke topology. We create a policy by using Parameter-Operator-Condition definitions. In our example, all VNets have "spoke" in their name matches to policy. We do this by using the *Name* parameter, *Contains* operator, and *spoke* conditions. To preview resources that match your policy, click the Preview Resources button. Figure 21-36 verifies that two VNets match to the policy.

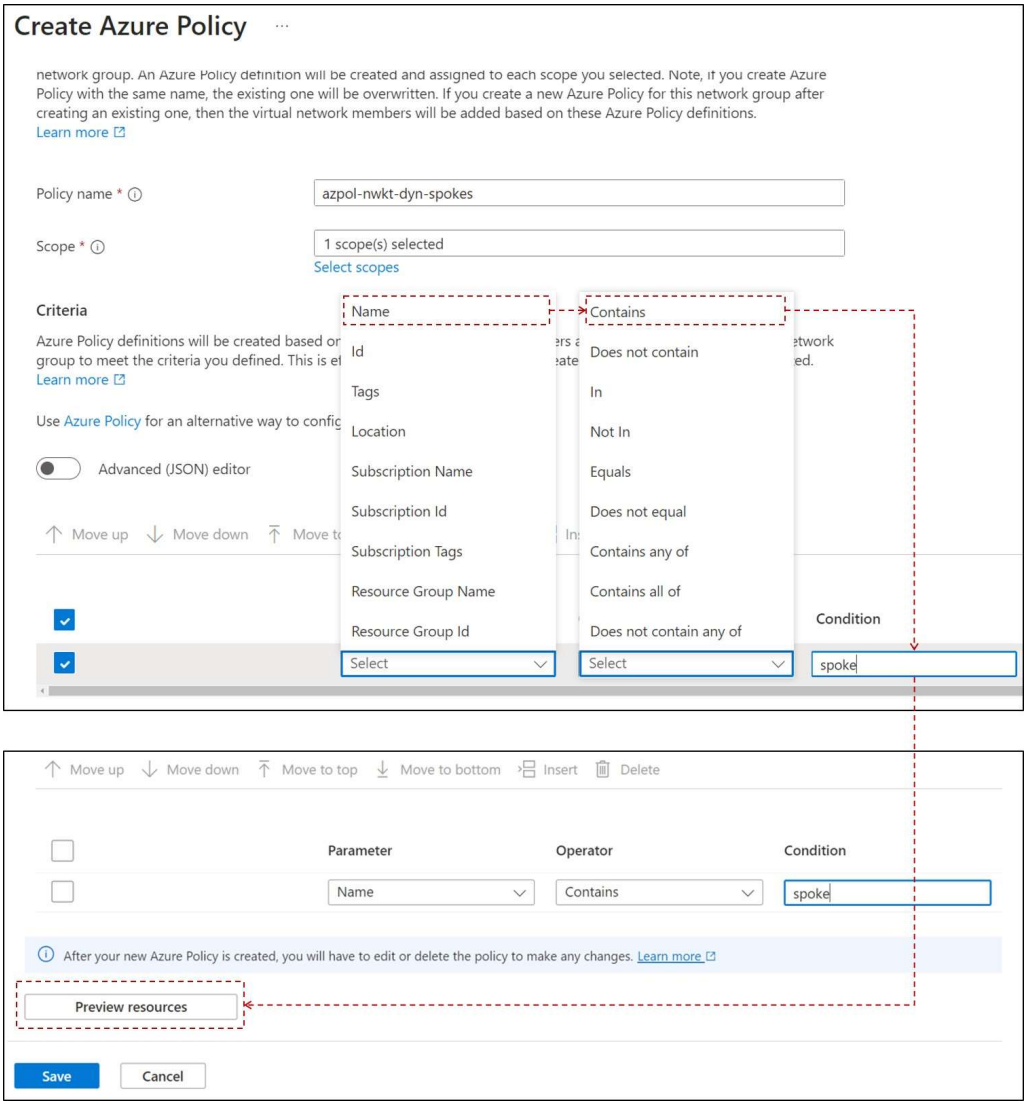

Figure 21-35: *Create Azure Policy – Define the Policy Rule.*

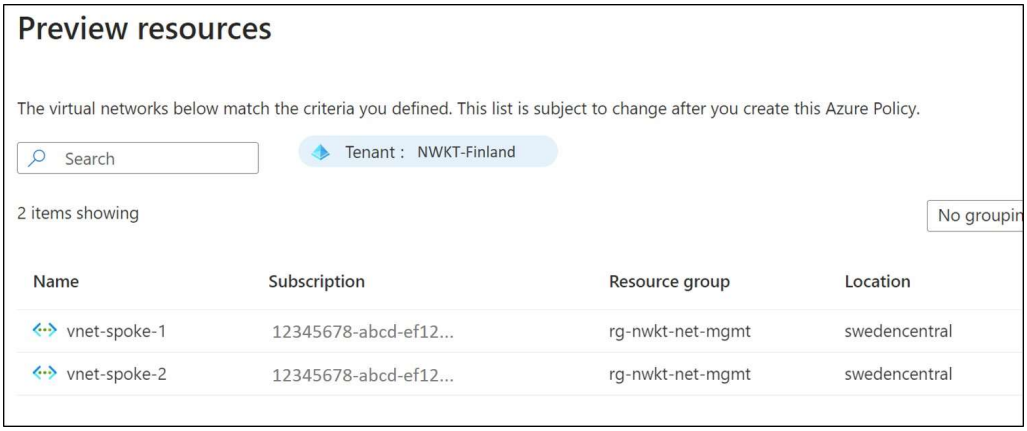

Figure 21-36: *Create Azure Policy – Preview Resources Matching the Policy Rule.*

Figure 21-37 illustrates how the new vnet-spoke-3 increases the *Number of members* listed by one. Figure 21-38, in turn, shows that it is automatically added to the Group Member list based on the policy.

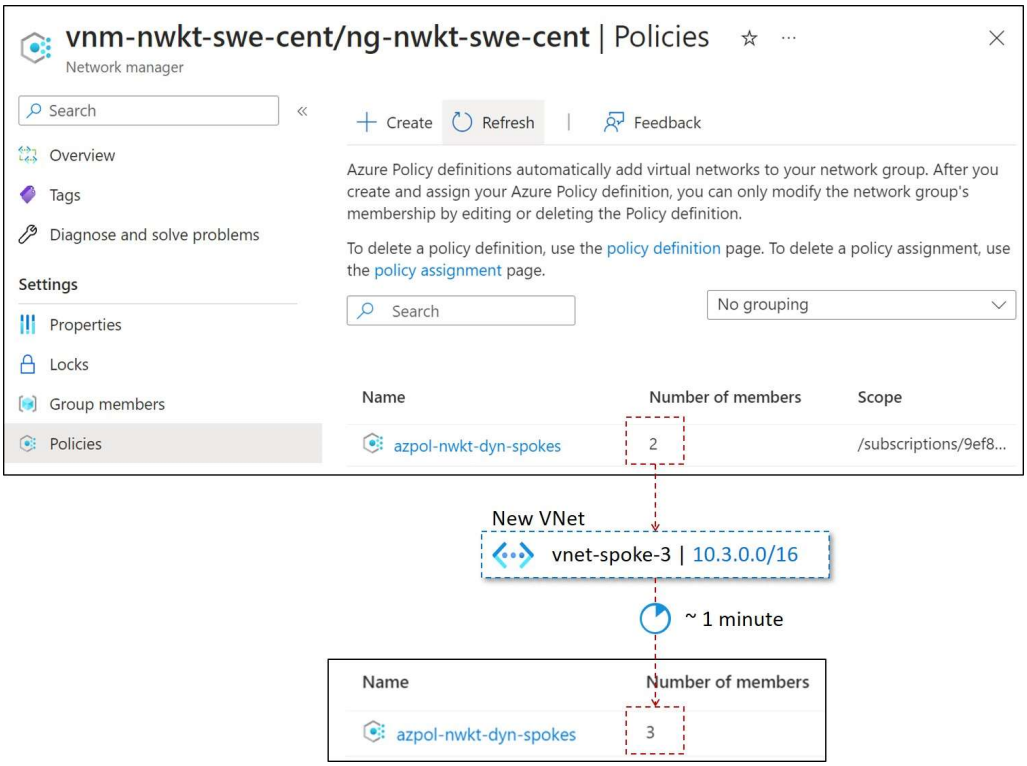

Figure 21-37: *Adding the VNet VNet vnet-spoke-3.*

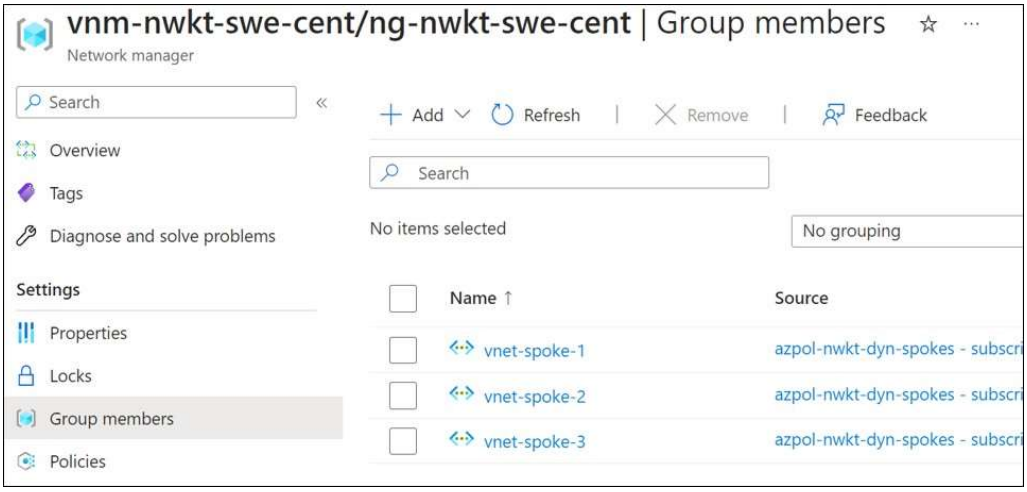

Figure 21-38: *Dynamic Group Members.*

Configuration and deployment processes are the same for manually added and policy-based Network Groups.

Verification

Figures 21-39 on the next page shows effective routes for vNIC vm-hub-1593 (vm-hub-1). It has learned all spoke VNet subnets over VNet peering connections. Figure-22-40, in turn, shows that vNIC vm-spoke-1768 attached to vm-spoke-1 has learned only the network 10.0.0.0/16 (vnet-hub) over VNet peering. The ping example below verifies that vm-spoke-1 has IP connectivity to VMs in vnet-hub but not with any other spoke VNets.

```
azureuser@vm-spoke-1:~$ ping 10.0.0.4 (=> vm-hub1)
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
64 bytes from 10.0.0.4: icmp_seq=1 ttl=64 time=1.64 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=64 time=1.31 ms
64 bytes from 10.0.0.4: icmp_seq=3 ttl=64 time=1.26 ms
--- 10.0.0.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.263/1.401/1.635/0.166 ms

azureuser@vm-spoke-1:~$ ping 10.2.0.4 (=> vm-spoke-2)
PING 10.2.0.4 (10.2.0.4) 56(84) bytes of data.
--- 10.2.0.4 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2026ms
```

Example 21-1: *Ping from vm-spoke-1 to vm-hub-1 and vm-spoke-2.*

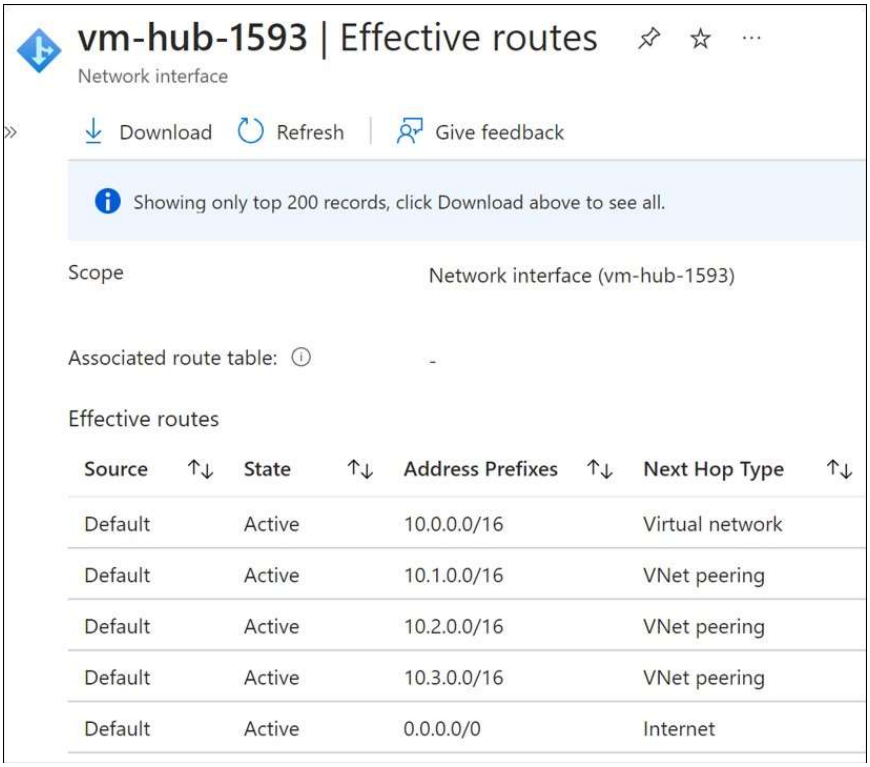

Figure 21-39: *Effective Routes of vm-hub-1539.*

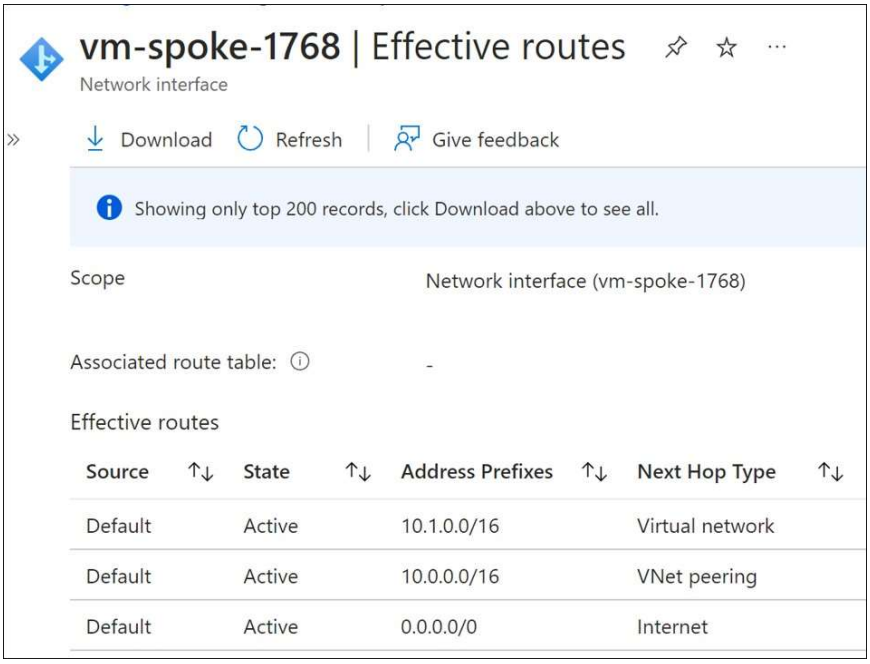

Figure 21-40: *Effective Routes of vm-spoke-1768.*

Delete Policy

Figure 21-41 depicts the Policy deletion workflow. The policy consists of two parts, Assignment and Definition. Assignment describes the scope of the policy while definition is the policy rule. Before deleting the policy rule (= policy definition), you must delete its assignment.

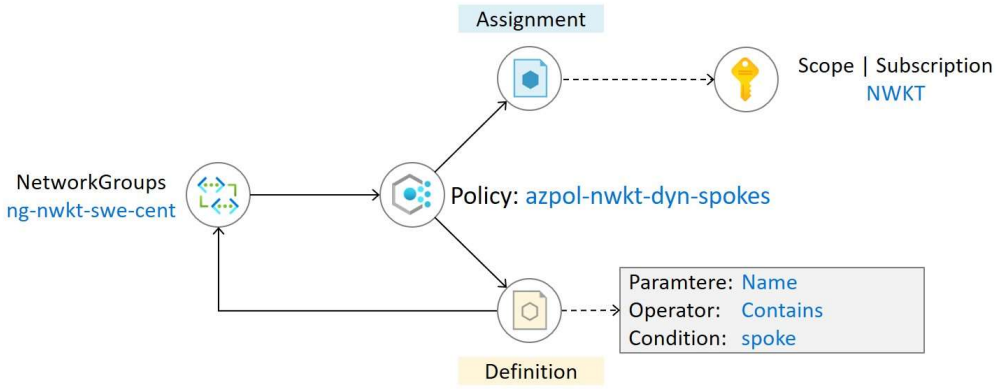

Figure 21-41: *Delete Azure Policy – Workflow.*

Start Azure policy deletion process by clicking the *policy assignment* hyperlink in the Policies window (Figure 21-42). It leads you to the Policy page (Figure 21-43).

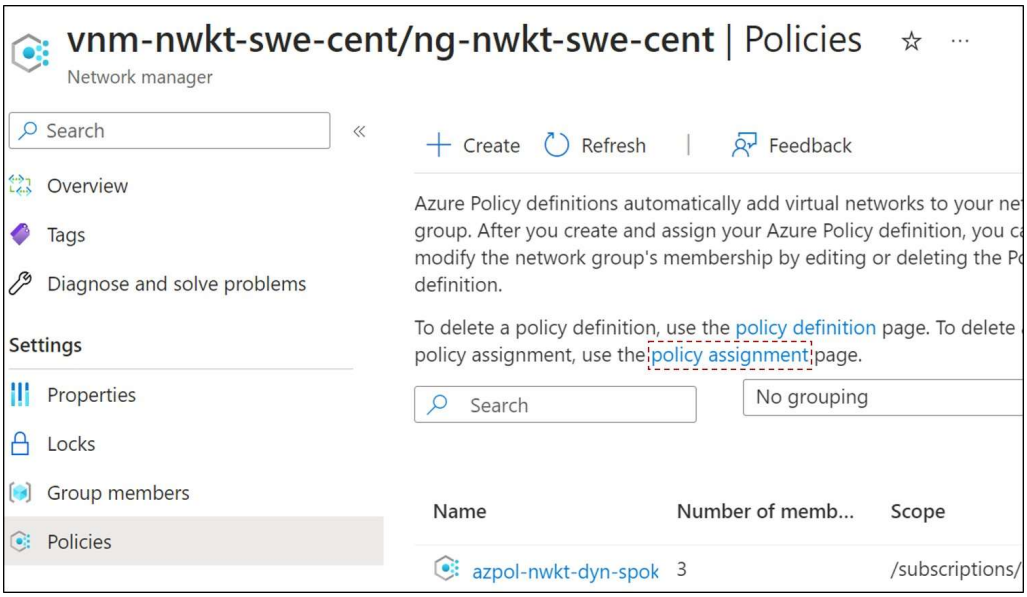

Figure 21-42: *Delete Azure Policy – Step#1: Delete Assignment (1).*

In the Policy Assignment window, click the assignment you want to remove (Figure 21-43).

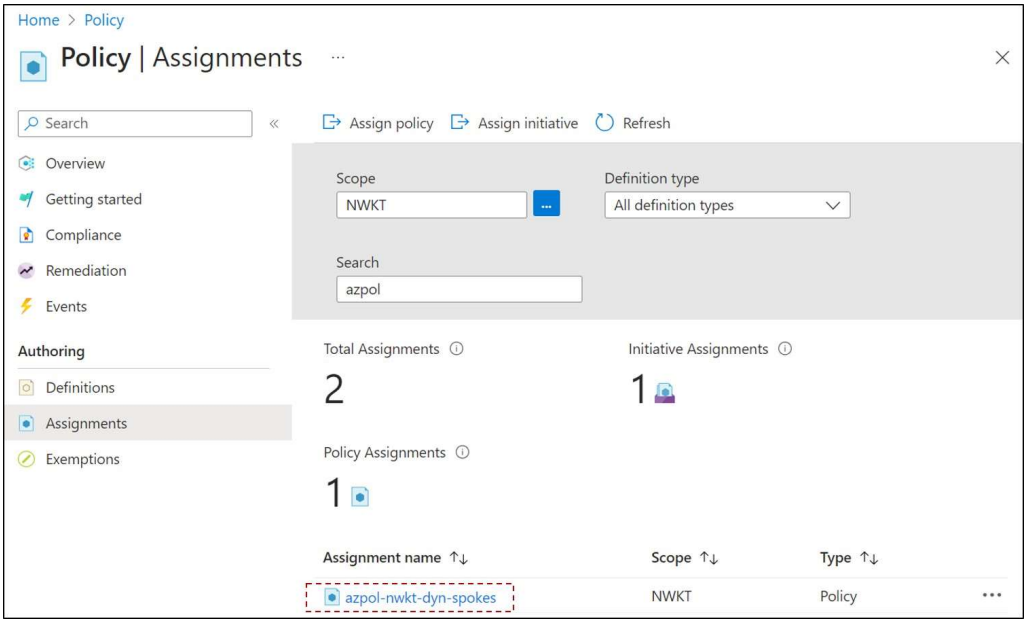

Figure 21-43: *Delete Azure Policy – Step#1: Delete Assignment (2).*

Then, click the Delete Assignment button on the menu bar (Figure 21-44).

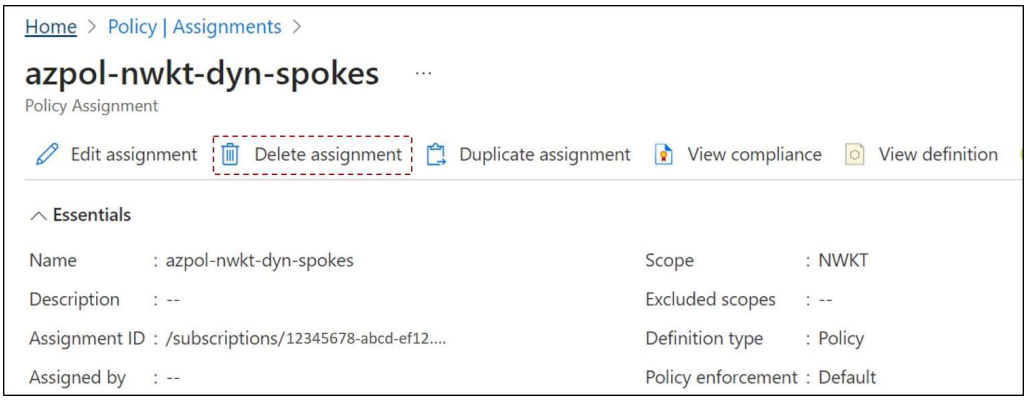

Figure 21-44: *Delete Azure Policy – Step#1: Delete Assignment (3).*

After deleting the policy assignment, select the policy definition you want to remove (Figure 21-45).

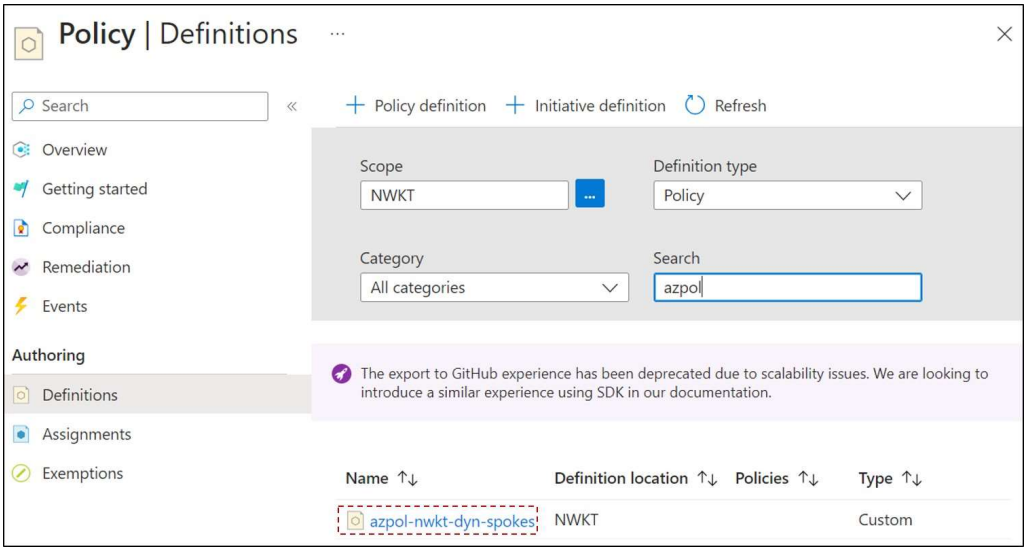

Figure 21-45: *Delete Azure Policy – Step#2: Delete Definition (1).*

Then, click the *Delete definition* button on the menu bar (Figure 21-46). Note that you can see the complete policy in JSON format after the *Essentials* section.

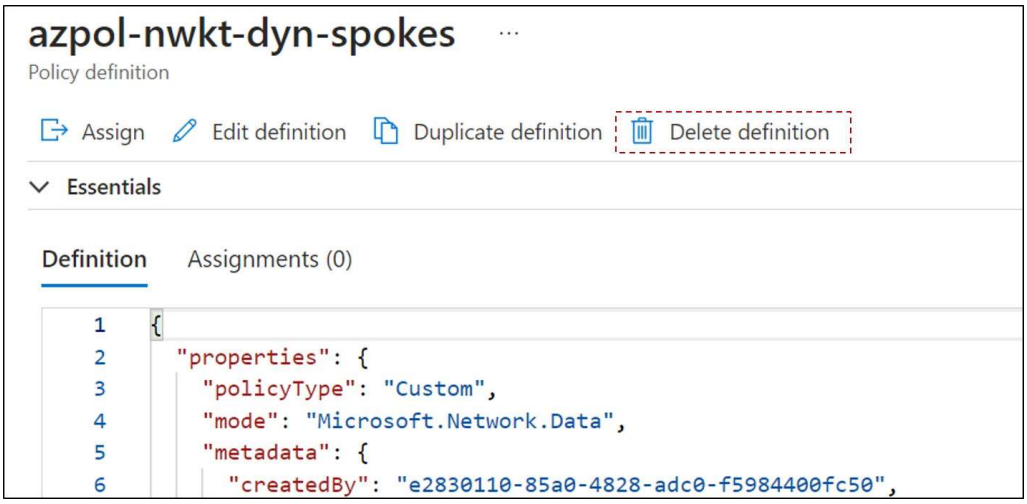

Figure 21-46: *Delete Azure Policy – Step#2: Delete Definition (2).*

Figure 21-47 verifies that we have successfully removed the policy.

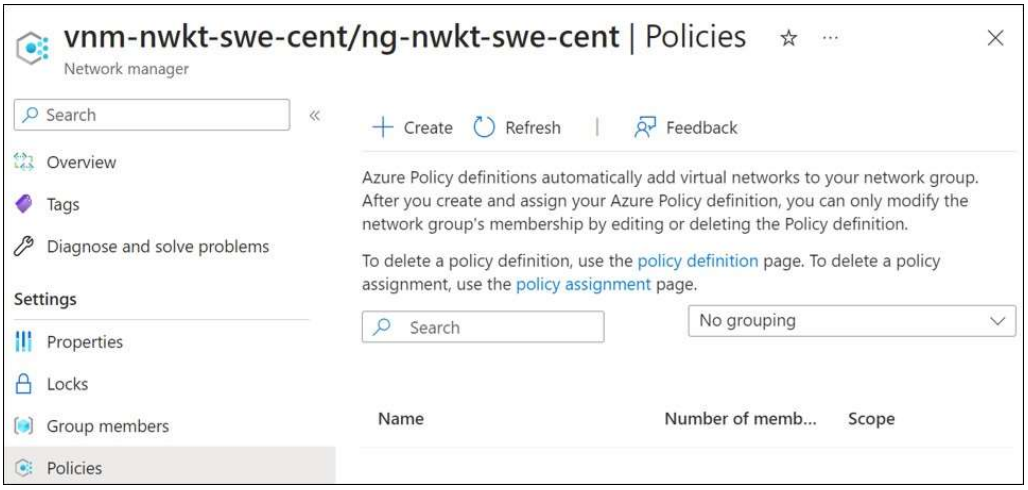

Figure 21-47: *Delete Azure Policy – Verification.*

Also, our spoke VNets are not listed in the Group Member windows (Figure 21-48). Figure 21-49, in turn, shows that all VNet peering connections are gone when deleting the policy.

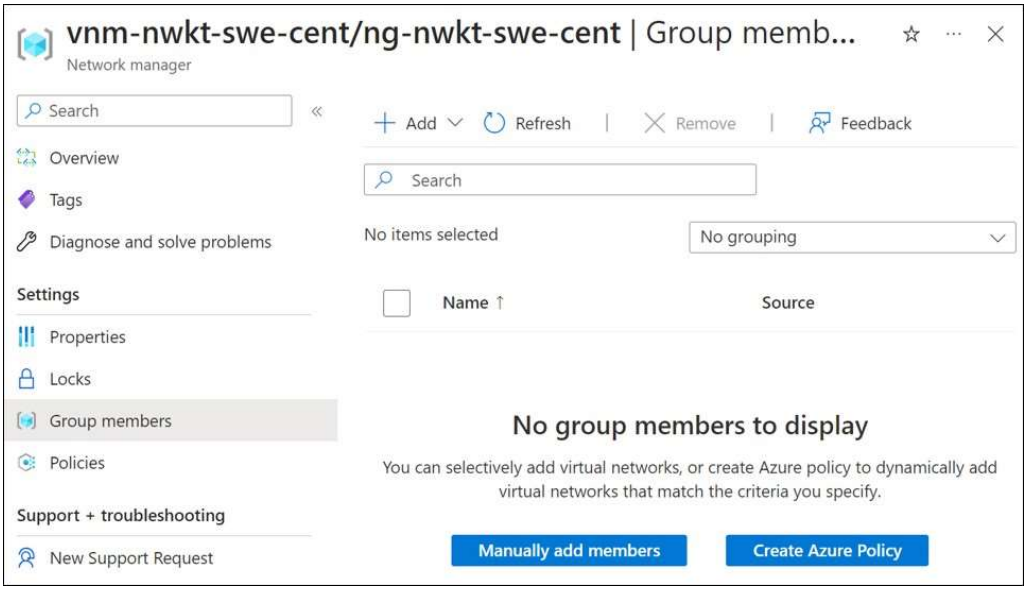

Figure 21-48: *Delete Azure Policy – Verification: Group Members.*

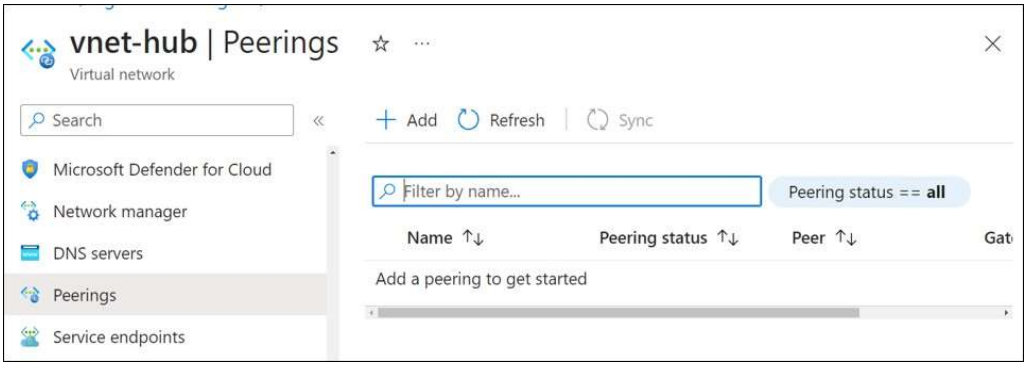

Figure 21-49: *Delete Azure Policy – Verification: VNet Peering Connections.*

Pricing

At the time of writing, the Azure Virtual Network Manager costs 0,092€ per hour. Check the latest pricing in your region from the Azure Pricing page.